UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 13-CR-155

JEFFREY FELDMAN,

Defendant.

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO COMPEL DISCOVERY AND DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The United States of America, by and through its attorneys, James L. Santelle, United States Attorney, Karine Moreno-Taxman, Assistant United States Attorney, and Jeffrey Zeeman, Trial Attorney, United States Department of Justice Child Exploitation and Obscenity Section, hereby submits the following response to defendant Jeffrey Feldman's "Motion to Compel the Government to Disclose the Computer Program Roundup, Its Manual and Protocols , and Its Technical Specifications" and his "Motion to Suppress" filed on January 6, 2014. (Doc. #25 and 26)

I. PROCEDURAL AND FACTUAL BACKGROUND

Background on P2P file-sharing and eMule[1]

During June-July 2012, an FBI online covert law enforcement agent conducted an undercover investigation into the distribution of child exploitation materials through peer-to-peer

[1] Much of this general background on P2P file-sharing and eMule is described in detail in the Affidavit of Robert Erdely, Ex. B hereto.

(P2P) file sharing networks. In this particular investigation, the undercover FBI agent investigated IP addresses using the peer-to-peer software called eMule, which shares files through the Donkey2000 (eDonkey) and Kademlia (KAD) P2P networks. Any member of the public can freely obtain this software by downloading it from an Internet website.

Peer-to-Peer (P2P) file sharing programs allow users to directly connect to other users on the same P2P network to transfer files through the Internet. Many of these programs, including eMule, are available free of charge to Internet users. Any files stored in a P2P user's shared directory are available for download by any other user of the same file sharing network.

Files that the user wants to share are placed by the user, via the eMule software, into shared folders in eMule. Both the eDonkey and KAD servers (the "eDonkey/KAD network" herein) act as an index which is searchable by other users of this file sharing network. eMule has the ability to locate files based on hash values[2] and to locate clients based on client hash numbers (a unique number provided by eMule to each IP address which uses eMule). The eDonkey/KAD network uses a variation of the MD4 algorithm called the eD2k MD4 to calculate hash values of files offered to the public in shared folders. These hash values are made available to the public

[2] A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 546-47 (D. Md. 2007). The most commonly used algorithms will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. *Id.* SHA-1 stands for Secure Hash Algorithm Version 1, and is one such commonly used hash algorithm. *United States v. Glassgow*, 682 F.3d 1107, 1110, n. 2 (8th Cir. 2012). Changing even one pixel in an electronic file will result in that file generating an entirely unique hash value; thus, any two files bearing the same hash values will be identical in all respects. Accordingly, courts regularly rely upon hash-matching evidence, including in the search warrant context. *See, e.g., Glassgow*, 682 F.3d at 1110 (crediting expert testimony that there is a 99.99999 percent probability that any two files sharing a SHA-1 value will be identical). *See generally United States v. Miknevich*, 638 F.3d 178, 184 (3d Cir. 2011) (holding that although the investigating officer never viewed the alleged images of child pornography on the defendant's computer, the warrant application provided sufficient probable cause where the highly descriptive names of the file contents indicated child exploitation files and the SHA1 values for those files matched SHA1 values of files known to contain child exploitation files).

on the KAD indexing servers. (See Erdely Affidavit Ex. B at paragraph 8 and Search Warrant Affidavit, Ex. A hereto at ¶ 7.).

For each file being shared, the user publishes the following information to the indexing server: file name; file size; hash value; user's IP address; and port. The indexing server stores this information and makes it available to other users on the network seeking similar files. (See Erdely affidavit, Ex. B hereto at paragraph 5). The file sharing network is designed to allow users to query the indexing servers by either keyword or hash value of files being shared on the network. The indexing server then responds with a list of file names that match the characteristics queried, allowing the user to select the file(s) desired to download. The indexing server then provides the user a list of IP addresses and port numbers that are sharing the desired file. The user's software then initiates a multi-source download directly from those IP addresses and ports. No portions of the file are stored on or received by the indexing servers. (See Erdely Affidavit, Ex B hereto at paragraph 7).

Background on the *RoundUp eMule* law enforcement tool

The undercover FBI agent was investigating IP addresses involved in making child exploitation files available to the public through the use of the eMule program. During this pre-search-warrant investigative stage, the undercover agent used the *RoundUp eMule* software. *RoundUp eMule* is nothing more than an investigative tool used to ascertain that a particular IP address was offering to share child exploitation material through the eDonkey/KAD network. (see Erdely Affidavit at paragraph 13). *RoundUp eMule* is a simple tool, which is simple to understand. It was designed to enable law enforcement to efficiently identify users sharing child exploitation files with the general public, while preventing law enforcement from accidentally

sharing contraband files. Although part of *RoundUp eMule's* name includes the word "roundup", it is not identical to the law enforcement tools used for other P2P programs such as Roundup Gnuettela, Roundup Bitorent, and Roundup Ares. These other tools were each independently developed with wholly distinct underlying programming architecture, even though much of the functionality is similar. Therefore, the defendant's reliance on training materials, white papers, or other resources that are not specific to *RoundUp eMule* is misplaced.

RoundUp eMule can only identify the IP addresses of a computer that had previously downloaded eMule and which had been configured to allow file sharing via the eDonkey/KAD file sharing network. *RoundUp eMule* allows law enforcement officers to query the eDonkey/KAD indexing servers by either keyword or the hash value of files being shared on the network. These search functions are paramount to a law enforcement investigation, as they allow searches to be conducted without requiring law enforcement to share contraband files depicting child exploitation. (See Banner Affidavit, Ex C hereto at paragraph 8). The software program does not perform any search of information stored on the computer identified via IP address. Instead, the program communicates with the indexing servers that are part of the publicly available eDonkey/ KAD network.

Although *RoundUp eMule* operates, in large part, precisely the same as the standard eMule software, it does feature some modifications designs to assist the investigative process. For example, *RoundUp eMule* creates reports, logs, and notes of the investigator's actions in a manner that can be viewed, and reviewed in the future. *RoundUp eMule* records all of the data it receives in log files, unlike the publicly available eMule program, which does not record all information it receives. As another example, *Roundup eMule* only allows for single source downloads, in other words, *Roundup eMule* only allows files to be downloaded from one user.

(See Erdely Affidavit Ex B at paragraph 17). *Roundup eMule* also allows an investigator to enable a fake file-sharing feature, to appear as if the program is sharing contraband child exploitation materials. The program prohibits, however, sharing of any such files with any third-party eMule user. (See Erdely Affidavit at paragraph 17). *RoundUp eMule* can leave only one type of data on a remote user's computer: a virtual "tag" that verifies that the two computers were in communication. This type of "tagging" feature is not unique to *RoundUp eMule*, but rather, is consistent with how P2P programs generally operate. (See Erdely Affidavit at paragraph 19).

When a law enforcement officer queries the files shared with the public on the eDonkey/KAD network, the results often reveal eMule users sharing child exploitation material that are not located in the officer's jurisdiction. Generally officers focus their time on those offenders located within their jurisdiction and take no further investigative steps for the IP addresses located outside their jurisdiction. To enable officers to effectively share these query results with law enforcement officers in the appropriate jurisdictions, the query results are stored in a database made available to law enforcement. This database allows law enforcement to identify targets in their jurisdiction, such as Jeffrey Feldman, who were identified as sharing child exploitation material. (See Banner Affidavit Ex. C at paragraph 7).

The Investigation and Search Warrant

As part of the undercover operation, the KAD network identified IP address 65.30.43.173 as offering for distribution over a dozen files with the identical hash values of known child exploitation files. Not all of *RoundUp eMule*'s above-described features are utilized in any particular pre-warrant investigation. In this particular case, the undercover FBI

agent did not enable fake file sharing and was unable to complete a single source download. (See Banner Affidavit Ex. C at paragraph 9). At no time did the undercover agent attempt (let alone succeed) to remotely access and/or gather information from the defendant's computer that was not otherwise made available to the public through the defendant's use of eMule's file-sharing function. (See Banner Affidavit Ex. C at paragraph 10).

On January 22, 2013, FBI Special Agent Brett Banner obtained a search warrant to search Jeffrey Feldman's residence. In support of the search warrant, Special Agent Banner submitted a 9-page affidavit setting forth the basis for probable cause to believe that the target residence concealed evidence relating to the distribution and possession of child exploitation files. (*See* Ex. A.). The search warrant affidavit explained the basis for probable cause to believe that evidence of a violation of 18 U.S.C. § 2252A would be located at Feldman's residence, as described below. The information included was based on Special Agent Banner's investigation as well as information provided to him by other law enforcement personnel, including an FBI Online Covert law enforcement agent (the "undercover agent"). (Ex. A. ¶ 5, 7). Special Agent Brett Banner, an experienced and trained law enforcement officer stated in the affidavit that it "was being submitted for the limited purpose of securing a search warrant and … did not set forth every fact related to or otherwise the product of this investigation." (Ex. A ¶ 5). The affidavit described the significance of IP addresses and hash algorithms in identifying child exploitation files and distributors, how P2P networks operate, and the meaning of Globally Unique Identifiers and computer ports. (Ex. A ¶¶ 7-13).

The affidavit discussed the results of this particular investigation. Specifically, between June 10, 2012 and July 24, 2012, an FBI agent, while connected to the Internet in an undercover

capacity, conducted numerous online investigations to identify individuals possessing and sharing child exploitation files using the eDonkey/KAD networks. (Ex. A ¶ 7). The undercover agent utilized a P2P file sharing program that queried the network to ensure that downloads occur only form a single selected source. *Id.* During those investigations, the undercover officer discovered, based on matching hash values to a law enforcement database of previously-identified child exploitation files, that IP address 65.30.43.173 made 17 files containing child exploitation material available to the public; all of which were files appearing to be related to child exploitation material. The hash values of those files were converted to the SHA-1 format and submitted to the National Center for Missing and Exploited Children, which verified that five of the files depicted known child exploitation victims. (Ex. A ¶ 10). For example, one file depicts, among other sexual acts, a prepubescent child performing oral sex on an adult male. A second file depicts, among other sexual acts, a prepubescent child masturbating. *Id.*

After the IP address was identified, law enforcement continued their investigation, as summarized in the search warrant. These additional investigative steps required significant resources and work to be done in order for the FBI to seek a search warrant. For example, the undercover law enforcement agent used Maxmind.com to determine that the IP address was registered to Time Warner /Road Runner. An administrative subpoena was issued by the FBI to Time Warner /Road Runner for the location and subscriber of the IP address during the undercover investigation. Time Warner reported that the IP address was assigned to Jeffrey Feldman, located at 2051 S. 102nd Street, apt. E., West Allis, Wisconsin, which was within the investigative jurisdiction of the undercover officer. Through additional investigation, law enforcement verified that this was indeed the correct address. In addition; they visited the

location and checked for any unsecured wireless connections. Law enforcement's review of administrative subpoenas and public records resulted in the affiant establishing that IP address 65.30.43.173 resolved to the defendant, Jeffrey Feldman. (Ex. A ¶¶ 9, 13-16 and Banner Affidavit at 17)

After reviewing the search warrant affidavit signed by FBI Special Agent Bret Banner Magistrate, Judge William Callahan signed a search warrant on January 22, 2013, authorizing the search of Feldman's residence. On January 24, 2013 law enforcement executed the search warrant for the computer and premises and seized a desk top computer and numerous encrypted hard drives and related contraband. They also conducted a short interview of Feldman[3] and conducted preliminary forensic analyses of the computers, which was in large part thwarted by the inability to access the encrypted electronic storage equipment.

The FBI was subsequently able to decrypt two of the hard drives. Based on the forensic analysis of the desktop and the two decrypted drives, a criminal complaint was issued. On August 20, 2013, a federal grand jury sitting in this district returned a six count indictment against Feldman charging him with five counts of receipt of child pornography and one count of possessing child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and (a)(5)(B). Feldman was arraigned and entered a plea of not guilty to all six counts. These charges were overwhelmingly grounded in information derived from the forensic analysis of Feldman's computer and hard drives. Eventually, agents succeeded in decrypting all of Feldman's electronic storage devices, and discovered at least tens of thousands of child exploitation files stored on those devices, as well as evidence that he had been utilizing P2P software to obtain

[3] As soon as Feldman invoked his right to counsel all questioning stopped.

some of those files.[4] To the extent permitted by 18 U.S.C. § 3509(m), redacted copies the forensic evidence in this case has been provided to defendant in the format requested. In addition, defense counsel and his expert witnesses have been invited to view the enormous volume of forensic evidence containing contraband files as frequently as desired at FBI offices. (See Banner affidavit at paragraph 21). To date, although the defendant has had access to this forensic evidence, the defendant has not pointed to a scintilla of forensic evidence suggestive of any activity he claims could have been done by the government. The matter is assigned to United States District Judge Lynn Adelman for trial and to this Court for processing pretrial motions.

II. ARUGMENT

For the reasons discussed in detail below, Feldman's motion to compel discovery and his motion to suppress should be summarily denied by this court. The United States has fully complied with its discovery obligations pursuant to Fed. R. Crim. P. 16 via its extensive discovery productions to date, as well as by making freely available for defense review the enormous volume of forensic evidence seized from Feldman's residence. Moreover, Feldman has wholly failed to comply with the local rules and failed to show a "particularized need" for the items he claims the United States must be compelled to produce. In addition, even if he had shown a particularized need, many of his requests seek proprietary investigative tools protected by the law enforcement privilege.

Regarding his motion to suppress, Feldman has failed to make the required "substantial preliminary showing" necessary for this Court to hold the requested *Franks* hearing. Moreover, Feldman had no reasonable privacy interest in the child exploitation files that he made freely available to the general public, and the information contained within the search warrant affidavit

[4] The digital system located in Feldman's residence was capable of storing approximately 19 terabytes of data. In comparison, the United States Library of Congress is 10 terabytes in size. (See Banner Affidavit at 23.)

(which was primarily based upon observations of those publicly-shared files) easily exceeded the probable cause threshold for a search of Feldman's residence. As such, both of Feldman's motions must be denied.

A. **The Defendant's Motion to Compel Should be Denied.**

1. The defendant failed to comply with local discovery rules.

On August 26, 2012 this court entered a pretrial order in this case which stated in pertinent part:

> 1.c. Any discovery motion under Fed.R.Crim.P. 16(a) or 16(b) must be accompanied by the statement required by Criminal L.R. 16(b).

Defendant Feldman failed to comply with the local rule, and the discovery already provided obviates the need for the requested discovery. *See United States v. Kelly*, 120 F.R.D. 106 (1987)).

Extensive discovery has been provided to the defense during the course of this investigation. The items include, among other things, numerous FBI reports, all requested logs pertinent to this investigation generated by *RoundUp eMule*, CDs containing more than a dozen forensic reports, hash value conversion charts, and the November 18, 2013 detailed letter. (The cover letters for the discovery provided are attached as Exhibit D.) In addition, although not required by Rule 16, redacted copies of forensic evidence were also produced to the defendant in the specific format he requested. The United States has made freely available to defense counsel and his expert the voluminous forensic evidence (many terabytes worth) seized from Feldman's residence.

Moreover, by way of a detailed letter dated November 18, 2013 (See Exhibit E), the United States answered many of Feldman's substantive interrogatory-style questions about the

technology involved in investigating this case, requested clarification on some of Feldman's other questions, and informed Feldman that it was willing to work with him on any additional discovery-related concerns. As part of this detailed letter, the United States informed the defendant that no "fake file sharing" occurred; the defendant's computer was not "tagged"; no screen shots were taken; no single-source download occurred; that there was no physical intrusion into his computer prior to the search warrant. Feldman did not take the United States up on its offer to further discuss discovery issues, nor did he provide the requested clarification about his numerous vague and/or confusing discovery requests. Instead, the defendant's motion to compel discovery is his third attempt to circumvent the local rules and the requirement that his counsel confer with the prosecution prior to bringing such motions.

First, on September 3, 2013, Feldman filed a motion although entitled "MOTION TO DESIGNATE THE CASE AS COMPLEX, MOTION FOR EXTENSION OF TIME TO FILE MOTIONS, AND MOTION FOR PRETRIAL SCHEDULING CONFERENCE**"** which was actually his first motion seeking court intervention in the discovery process (see Docket Document 12) in which he listed over 30 items sought in discovery. This motion was filed before the first (and only) Rule 16 Discovery Conference was held. Second, after the September 10, 2013 Discovery Conference, the defendant did not follow up with any requests or seek an additional Rule 16 Discovery Conference; rather, the defendant filed a motion on September 19, 2013 entitled "MOTION TO COMPEL" (see document 18) which listed a new long list of discovery demands. The United States objected to the defendant's motion for failure to comply with the local rules (see Document 19). On November 8, 2013 the United States produced to defendant additional information he had requested, and followed up with a detailed letter dated November 15, 2013, which, as discussed above, defendant

failed to respond to. On November 21, 2013, based on the United States' motion, this court denied the defendant's second motion to compel (without prejudice).

On the afternoon of January 3, 2014, Attorney Chris Donavon sent an email (See Exhibit F) stating that he was "writing pursuant to local Criminal Rule 16(b) to confirm that the government was denying the defense request for access to the Roundup program, its manual and protocols and its technical specifications under the claim of law enforcement privilege as asserted in the letter you sent Attorney Shellow on November 15, 2013.…" The United States again offered to meet and discuss the defense's concerns, and asked for the defense to "particularize exactly what you need…we can try to find a way to get you what you need, or at least clarify what we can and cannot provide." That email was unanswered. Instead, on January 6, 2014, the defendant filed a "Motion to Compel the Government to Disclose the Computer Program Roundup, Its Manual and Protocols, and Its Technical Specifications" (hereafter "Motion to Compel") seeking the disclosure of the "computer program Roundup, its manual and protocols, and its technical specifications."

The defendant should not be permitted to use the courts to sidestep the requirements of this district's local rules. From the onset, the defendant refused to avail himself of the United States' repeated offer to meet and discuss any discovery issues, which may have narrowed or resolved many of the issues he has instead chosen to raise via his third motion to compel.

2. <u>The United States has fully complied with Fed. R. Crim. P. 16 via its voluminous discovery production</u>.

Although Rule 16 requires the government to disclose, upon the defendant's request, all "documents ... within the government's possession, custody, or control ... [that are] material to preparing the defense," Fed. R. Crim. P. 16(a)(1)(E)(i), in order for a court to compel disclosure

"a defendant must make a threshold showing of materiality." *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995); *see also United States v. Ross*, 511 F.2d 757, 762 (5th Cir. 1975) (defendant must demonstrate that the sought after information bears more than some "abstract logical relationship to the issues in the case"). In doing so, "[n]either a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990); *see also United States v. Carrasquillo-Plaza*, 873 F.2d 10, 12-13 (1st Cir. 1989).

In his motion to compel, the defendant claims to need the requested items in order to determine whether "fake file sharing occurred", whether "tagging" was used, and whether the government intruded into the defendant's computer. The United States has already represented to defendant that none of these in fact occurred, and indeed, the *RoundUp eMule* program is not even capable of those types of tagging or intrusions. (See Erdely Affidavit at paragraphs 13-20). More importantly, defendant has not pointed to a scintilla of evidence derived from the enormous volume of forensic evidence in this case – which represents the overwhelming majority of evidence that will be introduced at trial – that suggests the investigation involved any tagging, fake file sharing or other type of invasion of the defendant's computer. Instead, he relies entirely on mischaracterizing out-of-context quotes from abstract academic articles that are totally unrelated to this investigation, and in most cases do not even relate to *eMule RoundUp*, the technology actually employed during this investigation. As such, his discovery request is nothing more than a speculative fishing expedition unsupported by any factual basis.[5]

[5] Beyond being wholly unsupported by any evidence related to this investigation, many of defendant's speculative theories are in fact flatly contradicted by the discovery produced to date. For example, the forensic examination of Feldman's electronic storage equipment demonstrates that numerous files identified in the search warrant were

In addition, Feldman raises novel claims which could have been muted if he simply communicated with the United States. For example, Feldman asserts that he needs additional discovery to support his claim that *RoundUp eMule* was never validated. However, the United States never received a request from the defense regarding whether a validation study had occurred. If the defense had so requested, he would have been informed that a validation study was completed by the MITRE Corporation. (See Erdely affidavit at paragraph 22). In all events, peer review is not required in order for law enforcement to use a tool such as *RoundUp eMule*. *See United States v. Chiardio*, 648 F3d 264(1st Cir. 2012)).[6]

The defendant seeks in his motion to compel several enumerated items under a claim that they are needed to properly attack the probable cause for the search warrant. The defendant, in support of his position, relies on the affidavit of Gerald R. Grant Jr. That affidavit fails to explain with any particularity how the disclosure of the "computer program Roundup, its manual and protocols, and its technical specifications" could potentially support his suppression argument. To the extent that any data obtained by RoundUp constituted an unlawful intrusion into a Fourth Amendment-protected arena, defendant and his expert can ascertain as much from the discovery provided to date, which includes: (1) all of the data (produced in log form) actually captured by *RoundUp eMule* pertinent to *this* investigation, (2) answers to all relevant questions about *RoundUp eMule*'s functionality, and (3) access to all of defendant's computer storage equipment, from which the expert could derive evidence about any purported intrusion by a government program. In addition, the defendant also seeks to have the court compel is needed in

---

downloaded onto the defendant's computer and/or hard drives prior to the dates of the undercover operation. Thus, it impossible to blame the undercover operation for such evidence being found on the defendant's computer and/or hard drives. This data clearly eliminates any claim of an government intrusion into Feldman's computer for the purpose of placing images and videos of child exploitation on Feldman's desktop and hard drives, or otherwise improperly inducing him to obtain child exploitation images. (See Banner Affidavit at paragraph 22).

[6] If this court finds it necessary, the United States would agree to allow for an in-camera review of the validation study.

order to determine whether he will seek a *Daubert* hearing to challenge the use of *Roundup eMule*. Such a claim is premature at this juncture of the case. No trial date has been set and neither party has filed a notice of expert as of yet.[7] Therefore, the defendant's claim for additional discovery based on the potential of a *Daubert* hearing is not ripe for review at this time and cannot form the basis for the disclosures the defendant seeks.

Next, the defendant requests information related to the hash values of the images found on the defendant's computer and hard drives. But, defendant has already been provided with the hash values of all the images identified in the search warrant, as well as those that are identified in the six count indictment returned against him. Defendant has no grounds for requesting the hash values of the hundreds of thousands of child exploitation images known to law enforcement, but not involved in this investigation. This enormous volume of information is simply immaterial to this case, and also law enforcement sensitive. (See Erdely Affidavit at paragraphs 23-24). Finally, to the extent he so desires, defendant's own expert can easily ascertain the hash values of any of the many thousands of child exploitation files located on defendant's computer storage system, which he has full access to, and which include some of the files he was initially detected making available via a P2P network. Had the defendant sought this information from the United States, rather than through a motion to compel, the United States would have directed him to publicly available software that he can use to perform his own hash conversion. (See Erdely Affidavit at paragraph 8).

3. <u>RoundUp eMule and its library of hash values are protected by the law enforcement privilege</u>.

[7] Moreover, to the extent the defendant wants to challenge any such evidence presented by an expert, he can do so by cross examination, if such an expert is called. *United States v. Crisp*, 324 F. 3d 261 (4th Cir. 2003); *United States v. Hernandez-de la Rosa*, 666 F. Supp. 2d 175 (D.P.R. 2009); *United States v. Lauder III* (10th Cir. 2005).

Assuming arguendo, that the defendant has satisfied the threshold showing required for establishing his need for the items he seeks and that they are material to preparing his defense, the law enforcement privilege provides for further protection from compelled disclosure of the tool's protocols, manuals etc.. The defendant has failed to "demonstrate an authentic necessity, given the circumstances, to overbear the qualified privilege." *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987). The affidavit of Robert Erdely invokes the law enforcement privilege on behalf of the FBI. (See Erdely Affidavit at paragraphs 24-25).

The law enforcement privilege protects sensitive investigative techniques, such as the type and precise location of equipment used in electronic surveillance, *United States v. Van Horn*, 789 F.2d 1492, 1507-08 (11th Cir. 1986) and *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987); information concerning the location of posts used by surveillance agents, *United States v. Harley*, 682 F.2d 1018, 1020-21 (D.C. Cir. 1982) and *United States v. Green*, 670 F.2d 1148, 1155 (D.C. Cir. 1981); an agency's investigatory files or information regarding those files, *Raz v. Mueller*, 389 F.Supp.2d 1057, 1061-62 (W.D. Ark. 2005); reports made by undercover agents, *In re The City of New York*, 607 F.3d 923, 928-29 (2d Cir. 2010), and other aspects of law enforcement operations. The purpose of the privilege "is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." *In re Dep't of Investigation*, 856 F.2d 481, 484 (2d Cir. 1988); *Commonwealth of Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007). "Just as the disclosure of an informer's identity may destroy his future usefulness in criminal investigations, the identification of a hidden observation post will

likely destroy the future value of that location for police surveillance." *Green*, 670 F.2d at 1155; *Cintolo*, 818 F.2d at 1002, n.13 (holding the privilege protects secret surveillance information).\

Here, the law enforcement privilege should protect the government from being compelled to disclose the items the defendant seeks. Roundup eMule is a law enforcement tool which is deserving of protection pursuant to the law enforcement privilege. Law enforcement had a great a deal of difficulty in the past identifying those using P2P networks to distribute, receive, and possess child exploitation files. The disclosure of the computer program Roundup, its manual and protocols, and its technical specifications sought by the defendant would chill law enforcement investigations of such offenses as the materials the defendant seeks could be used by offenders to either evade apprehension or to mislead the authorities. (See Erdely Affidavit at paragraphs 23-24). Access to these items would allow perpetrators of these crimes, many of whom (like the defendant) are very knowledgeable regarding computers to impede future law enforcement investigations. For example, knowing the specifics the defendant seeks to have disclosed to him of the *RoundUp eMule* tool would allow others to reveal what programs and protocols to look for when using P2P networks so as to avoid law enforcement detection. *Id.* Once offenders know which files (identified by hash value) law enforcement is aware of, they can easily modify the image by one pixel so that it would have a new and unknown hash value, despite appearing the same to the naked eye. This newly created hash value would be unknown to law enforcement and thus could no longer be detected. Similarly, if *RoundUp eMule*, its manual and protocols, and its technical specifications were disclosed criminals, could purposely avoid law enforcement by avoiding searching for those images or by publishing lists of images sought by law enforcement.

Numerous courts have employed a ten-factor balancing test to determine if the information sought falls under a law enforcement privilege. *See, e.g., In re U.S. Dep't of Homeland Sec.*, 459 F.3d 565, 570-71 (5th Cir. 2006) (referring to the 10-part standard as the "Frankenhauser test," after *Frankenhauser v. Rizzo*, 59 F.R.D. 339, 344 (E.D. Pa. 1973)). The Frankenhauser test examines: (1) the extent to which disclosure will thwart governmental processes by discouraging citizens from giving the government information; (2) the impact upon persons who have given information of having their identities disclosed; (3) the degree to which governmental self-evaluation and consequent program improvement will be chilled by disclosure; (4) whether the information sought is factual data or evaluative summary; (5) whether the party seeking discovery is an actual or potential defendant in any criminal proceeding either pending or reasonably likely to follow from the incident in question; (6) whether the police investigation has been completed; (7) whether any intradepartmental disciplinary proceedings have arisen or may arise from the investigation; (8) whether the plaintiff's suit is non-frivolous and brought in good faith; (9) whether the information sought is available through other discovery or from other sources; and (10) the importance of the information sought to the plaintiff's case. *Id.*; see also *Tuite v. Henry*, 98 F.3d 1411, 1417 (D.C. Cir. 1996) (ordering district court to use the *Frankenhauser* test). The computer program, manual and protocols, and technical specifications for *Roundup eMule* are entitled to the law enforcement privilege, pursuant to the factors described in *Frankenhauser*.

In sum, the defendant's motion to compel should be summarily denied as the defendant has failed to follow the local rules, failed to show a particularized need for the requested

materials as required by Fed. R. Crim. P. 16, and has failed to overcome the law enforcement privilege asserted in this case.

B. Feldman's Motion to Suppress Should be Denied

1. Feldman is not entitled to a *Franks* hearing

In his motion, Feldman contends that the evidence seized during the search of his residence on January 24, 2013 must be suppressed because of a defect in the search warrant affidavit. Specifically, Feldman contends that the affidavit "did not sufficiently allege probable cause and therefore the search warrant should not have issued." Arguments and Authorities in Support of Motion to Suppress ("Motion to Suppress Memorandum") (Doc. #27), p.1. Feldman also contends that the affidavit "contained material omissions and false information," and requests an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978) in order to bolster this assertion. *Id.* He therefore requests a *Franks* hearing on the theory that the warrant "contains reckless omissions that were material to the finding of probable cause."

In order for Feldman to be entitled to a *Franks* hearing, he "must make a 'substantial preliminary showing' that: (1) the affidavit contained a material false statement; (2) the affiant made the false statement intentionally, or with reckless disregard for the truth; and (3) the false statement was necessary to support the finding of probable cause." *See United States v. Maro*, 272 F.3d 817, 821 (7th Cir. 2001) (quoting *Franks*, 438 U.S. at 155-56). Allegations that the affidavit omitted material statements are subject to the same standard. *See United States v. Williams*, 737 F.2d 594, 604 (7th Cir. 1984).

The burden on the movant in seeking a *Franks* hearing is "substantial." *United States v. Johnson*, 580 F.3d 666, 670 (7th Cir. 2009). "[A]ffidavits supporting a search warrant are presumed valid, and . . . the 'substantial preliminary showing' that must be made to entitle the defendant to an evidentiary hearing must focus on the state of mind of the warrant affiant, that is the police officer who sought the search warrant." *United States v. Jones*, 208 F.3d 603, 607 (7th Cir. 2000) (citing *Franks*, 438 U.S. at 171). "The defendant must offer evidence showing either that the warrant affiant lied or that the warrant affiant recklessly disregarded the truth because he 'in fact entertained serious doubts as to the truth of his allegations' or had 'obvious reasons to doubt the veracity of the allegations.'" *Id.* (citing *Williams*, 737 F.2d at 602); *see also generally United States v. Bershchansky*, Case No. 12-CR-00064, 2013 WL 3816570 (E.D.N.Y. July 19, 2013) (denying request for *Franks* hearing in challenge to child exploitation search warrant affidavit, noting "[t]o avoid 'fishing expeditions into affidavits that are otherwise presumed truthful . . . [the defendant] should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons.'" (quoting *United States v. Falso*, 544 F.3d 110, 125-126 (2d Cir. 2008)). Negligence by the affiant does not constitute reckless disregard for the truth. *See United States v. A Residence Located at 218 Third Street*, 805 F.2d 256, 258 (7th Cir. 1986). With this in mind, "*Franks* hearings are rarely required." *Johnson*, 580 F.3d at 670 (citing *Maro*, 272 F.3d at 821).

a. Feldman fails to make a "substantial preliminary showing" that the search warrant affidavit included a false statement or omitted a material fact.

In his motion, Feldman first asserts that the search warrant affidavit contains information that is "not true" because the program *RoundUp eMule* "conducted the investigation," which was not disclosed in the affidavit. Motion to Suppress Memorandum, p. 5. It is this assertion, rather

than any omission from the search warrant, which is in fact misleading. The affidavit accurately disclosed that an undercover officer conducted the investigation with the assistance of an enhanced "P2P file sharing program …." (Ex. A, ¶ 7). Importantly, the affidavit also disclosed additional investigative steps that were not performed by *RoundUp eMule*'s automated functions, including, for example, reviewing child exploitation files obtained from the National Center for Missing and Exploited Children which generated the same hash values as the files shared by defendant. (Ex. A., ¶ 10).[8]

Feldman also complains that omission of the "name and capacities of RoundUp … prohibit a magistrate from knowing whether Feldman was lured by the use of Honeypots."[9] As a matter of fact, Feldman was not "lured" by the use of so-called Honeypots because fake file sharing was not enabled during this investigation (See Banner Affidavit at paragraph 9), and Feldman admits that his argument on this point is entirely speculative, despite his expert's review of the forensic evidence seized from his residence ("Whether any versions of RoundUp ever did respond to source exchange requests is knowledge outside the purview of this writer," Motion to Suppress Memorandum, p. 7). But even if he had been so lured, Feldman's *motivations* for sharing child exploitation files do not constitute a "material fact." The search warrant affidavit accurately disclosed that Feldman was sharing with the general public (not just law enforcement), from a computer located at his residence, files that generated the same hash values as known child pornography files. The agents conducting the investigation confirmed that

[8] Feldman makes much ado about nothing in discussing a "pirate bay" and "supernode" located in Sweden. Motion to Suppress Memorandum pp. 5-6. First of, *RoundUp eMule* does not utilize supernodes as an index, and the "pirate bay" he discusses acts as an index on the bittorent file sharing network, and therefore was no relevance to this investigation. *See* Erdeley Aff. ¶ 6. Second, all P2P networks operate using third-party indexers on the Internet, and Brett Banner in fact disclosed in his affidavit that connections between devices on the Internet "often cross state and international borders," which would, of course, include Sweden. Ex. A, ¶ 6.b.

[9] More generally, Feldman offers no legal support for the novel argument that a search warrant is required to disclose the name and all the capabilities for any investigative tool used to gather some of the evidence that formed the basis for probable cause.

defendant was sharing child exploitation files, specifically describing two of those files in the search warrant affidavit. (Ex. A ¶ 10). The search warrant affidavit offers no speculation whatsoever regarding Feldman's motivation for sharing those files, nor is such motivation in any way material to a determination of whether there was probable cause that child exploitation files would be located at his residence.

Feldman also contends that the purported omission of the exact number of unsuccessful download attempts is a material omission warranting a *Franks* hearing. Motion to Suppress Memorandum, pp. 10-12. But again, the affidavit in fact candidly disclosed that the undercover officer "attempted without success to conduct single source downloads of the suspected child exploitation files from IP address 65.30.43.173." (Ex. A., ¶ 12). The Magistrate Judge was therefore fully aware that the undercover officer was unable to complete a single source download despite multiple attempts to do so, and made the probable cause determination with this fact in mind. Other courts have repeatedly found probable cause to search a residence based on hash matching, even without a successfully-completed download from a target's computer. *See infra* at pp. 31-32.

More importantly, the Seventh Circuit has pointedly held that *entirely* omitting unsuccessful investigative techniques from a search warrant is not improper. *See United States v. Singleton*, 125 F.3d 1097, 1102 n. 4 (7th Cir.1997) (officers do not have to include in an affidavit for a search warrant reports of unsuccessful attempts by informants to purchase drugs from a suspect); *United States v. McNeese*, 901 F.2d 585, 596 (7th Cir. 1990) (declining defense request for a *Franks* hearing where police officer located cocaine residue in the defendant's garbage, but failed to disclose that he subsequently searched the garbage several other times and

found no cocaine, because the omission was neither reckless nor deliberately false, and because even if the judge been aware of the unsuccessful searches, probable cause had been established by the one successful search of the garbage) (overruled on other grounds by *United States v. Westmoreland*, 240 F.3d 618, 632-33 (7th Cir. 2001)). *See also United States v. Wright*, 2009 WL 3358489 (10th Cir. Oct. 20, 2009) ("Inclusion of the details of Detective Reid's unsuccessful investigative techniques would not have altered the probable cause analysis in any way. Under the totality of the circumstances test, the affidavit in this case supports probable cause regardless of whether evidence of Detective Reid's failed knock and talks, trash covers, and controlled buys is included."); *United States v. Charles*, 138 F.3d 257, 263 (6th Cir.1998) (omission from search warrant affidavit that law enforcement officer made several unsuccessful attempts to purchase drugs from subject does not make the affidavit false or defeat probable cause); *United States v. Sugar*, 606 F.Supp. 1134, 1150–51 (S.D.N.Y.1985) (probable cause not vitiated by failure of officer to inform magistrate that undercover agent had been unsuccessful in attempt to obtain drug from defendants).

b. Feldman fails to make a substantial preliminary showing that the inclusion of the allegedly omitted Facts in the affidavit would negate a finding of probable cause.

Perhaps most importantly, Feldman fails to explain how any of the allegations in his motion are *material* to the finding of probable cause. An omitted fact is not material unless its inclusion would prevent the affidavit from supporting a finding of probable cause. *See Williams*, 737 F.2d at 604; *see generally Maro*, 272 F.3d at 821 (7th Cir. 2001) (noting that unimportant allegations, even if untrue or misleading, are not sufficient to trigger the need for a *Franks* hearing).

Here, the search warrant affidavit supports a finding of probable cause that Jeffrey Feldman's residence concealed evidence of violations of 18 U.S.C. § 2252A. Feldman's burden in seeking a *Franks* hearing is to make a "substantial preliminary showing" that the inclusion of the allegedly omitted fact(s) would destroy such a finding. Feldman is unable to meet this burden. Nothing in Feldman's motion calls into question key facts supporting probable cause, including: (1) agents conducted an investigation into the online sharing of child pornography through the eDonkey and Kademlia peer-to-peer network; (2) agents identified 17 files of suspected child exploitation files offered through those networks by a computer using the IP address 65.30.43.173; (3) agents learned that five of those files depicted known child exploitation victims; (4) agents visually confirmed that two of those files were videos of prepubescent children engaged in sexually explicit conduct; and (5) agents determined that Jeffrey Feldman was the subscriber associated with that computer and IP address. Under these circumstances, a *Franks* hearing would serve no purpose. *See United States v. Carmel*, 548 F.3d 571, 577 (7th Cir. 2008) ("[I]f probable cause to issue the warrant would still exist even if the false statement or material omission were corrected, then no *Franks* hearing is required.") (citing *United States v. Souffront*, 338 F.3d 809, 822 (7th Cir. 2003)).

c. Feldman fails to make a substantial preliminary showing that the affiant intentionally or recklessly omitted facts from the affidavit.

Finally, Feldman fails to address the requirement that he make a "substantial preliminary showing" that a material omission (whatever it may be) was made intentionally or with reckless disregard for the truth. In order to obtain a *Franks* hearing, Feldman's burden is to "'offer direct evidence of the affiant's state of mind or inferential evidence that the affiant had obvious reasons for omitting facts in order to prove deliberate falsehood or reckless disregard.'" *Souffront*, 338

F.3d at 822 (7th Cir. 2003) (citing *United States v. McNeese*, 901 F.2d 585, 594 (7th Cir. 1990), overruled on other grounds as recognized by *United States v. Westmoreland*, 240 F.3d 618, 632–33 (7th Cir. 2001)).

Here, Feldman provides no showing of falsity on the part of the affiant. While the many unsupported and conclusory allegations in the motion seem to point fault at "law enforcement" in general, there is nothing to indicate that the affiant lied or otherwise recklessly disregarded the truth in his affidavit. Indeed, Feldman has provided no evidence on this point; the reason he requests a *Franks* hearing is to try to fish for such evidence. (*See* Doc. #27 at 15 "Feldman requests a Franks hearing to show that agents made material omissions in the Affidavit in reckless disregard of the truth."). This approach conflicts with the limited purpose of a *Franks* hearing. *See Franks* 438 U.S. at 171; *United States v. McAllister*, 18 F.3d 1412, 1416 (7th Cir. 1994) ("[A]s the *Franks* Court went on to explain, to mandate an evidentiary hearing for the purpose of challenging a warrant affidavit, 'the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine' the affiant." (quoting *United States v. Radtke*, 799 F.2d 298, 310 (7th Cir. 1986)). As Feldman is unable to support his assertions, his motion must be denied.

As noted above, the affidavit is presumed to be valid, and the Seventh Circuit has repeatedly stated that "[c]onclusory, self-serving statements are not enough to obtain a *Franks* hearing." *Johnson*, 580 F.3d at 671 (citing *Franks*, 438 U.S. at 171); *see, e.g., United States v. Reed*, 726 F.2d 339, 342 (7th Cir. 1984) ("[T]he *Franks* presumption of validity of an affidavit supporting a search warrant cannot be overcome by a self-serving statement which purports to refute the affidavit." (citation omitted); *see also e.g., United States v. Collins*, 753 F. Supp. 2d

804, 811-12 (S.D. Iowa 2009) (noting inter alia that defendant's general assertions regarding law enforcement peer-to-peer investigative software were not sufficient to meet "substantial" burden required to obtain *Franks* hearing); *United States v. Hibble*, No. CR 05-1410, 2006 WL 2620349 (D. Ariz. Sept. 11, 2006) (denying defendant's request for *Franks* hearing based on alleged omissions in search warrant affidavit that discussed online investigation into sharing of child exploitation files on peer-to-peer network).

2. The investigation, including the use of RoundUp eMule, did not infringe upon Feldman's reasonable expectation of privacy.

Although not clearly articulated in his Motion to Suppress, defendant essentially argues that the government's use of *RoundUp eMule* during its investigation constituted an invasion of his privacy interest protected by the Fourth Amendment, notwithstanding the fact that defendant was publicly sharing all of the child exploitation files recorded by *RoundUp eMule*. In support of this argument, Feldman contends that *RoundUp eMule* was "developed to subvert the warrant requirement" by invading non-shared folders on the target's computers. Motion to Suppress Memorandum, pp. 7-10, 13-14. These contentions are neither true, nor relevant to his motion. Feldman supports his claims with misleading, out-of-context quotations from an article drafted not by attorneys or law enforcement investigators, but by computer scientists. Those same arguments, based on many of the same misleading citations, were recently rejected in persuasive fashion by other judges in this district. *See* Case Decision and Order (Ex. G hereto) at p. 6 ("[t]he articles [cited by defendant] provide no non-speculative basis for believing that RoundUp may e used to invade private spaces"); Recommendation and Order on Defendant Case's Motion to Suppress Evidence at p. 7 ("Case Recommendation") (Ex. H hereto) (concluding that "alleged 'high likelihood' that *RoundUp eMule* anonymously invades parts of the target computer other

than the file sharing program is completely speculative and, in fact, is contradicted by the evidence Case does cite. In one of the various articles cited by Case, the developers of *RoundUp eMule* explicitly state that their software 'does not allow law officers to hack into an individual's private computer.'") *See also* Affidavit of Robert Erdely, ¶ 15 ("*RoundUp eMule* cannot access any files or user information not made available to the public either through the user's shared folder or on the indexing servers").

Defendant states that *RoundUp eMule* "manipulates" an offender's computer, causing it to "return data that would not normally be available to the public." Motion to Suppress Memorandum p. 9. This is untrue. *RoundUp eMule* had no impact upon the data returned by Feldman's, nor any other offender's, computer. Instead, *RoundUp eMule* obtains data about files offered for distribution precisely as any other P2P program does, by seeking out files that an offender has widely broadcast to a public P2P network that he is making available to download. *RoundUp eMule* does not gather this information directly from defendant's computer itself, but rather, from a network index that collects this type of information from a variety of P2P users, and then shares that information with all users of the P2P platform. *See* Affidavit of Robert Erdely, ¶ 20.

In all events, Feldman's unsupported claims about the motivations of the computer programmers who developed *RoundUp eMule* have no bearing whatsoever on whether a *Franks* hearing is required based on actions and purported omissions of investigators using that program. And defendant's general claims about *RoundUp eMule*'s capabilities are wholly immaterial to defendant's motion to suppress, because his expert has not identified, during forensic review of Feldman's computers, any actual intrusion into his computer by *RoundUp eMule* itself. *Cf.* Case

Decision and Order (Ex. G hereto) at pp. 6-7 ("even if RoundUp could be used improperly, defendant makes no claim that the government invaded the private spaces of his computer, to insert tags or to search for evidence, despite the fact that he had forensic experts examine the computer") (emphasis in original).

The Supreme Court has repeatedly explained that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44, (1979); *Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection"). The lone case relied upon by defendant, *Kyllo vs. United States*, 533 U.S. 27, 40 (2001), which holds that the government may not explore details of a home that could not be viewed without physical intrusion, is not to the contrary. More specifically, the federal courts of appeals that have examined the privacy implications of searching P2P networks for files potentially containing child exploitation files have uniformly concluded that publicly available information does not violate a computer user's reasonable expectation of privacy. *See, e.g., United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir.2010) (rejecting the argument that the defendant had a reasonable expectation of privacy in files that were shared on a peer-to-peer file sharing site, regardless of defendant's intent to maintain the files as private). The *Borowy* court concluded that the use of a forensic software program unavailable to the public did not renders the search unlawful, and concluded that it did not. *See id.* (describing the software as "function[ing] simply as a sorting mechanism to prevent the government from having to sift, one by one, through [the defendant's] already publically exposed files"). *See also United States v. Norman*, 448 F. App'x 895, 897 (11th Cir.2011) (search of defendant's computer did not

constitute an unlawful search because information on shared folder was also available to members of the public); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir.2009) (defendant had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where Limewire made files accessible to other users); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir.2008) (defendant had no expectation of privacy in his subscriber information because peer-to-peer software permitted anyone else on the internet to access at least certain folders in his computer and such access could expose his subscriber information to outsiders.").

Even more pointedly, a federal district court recently determined that the RoundUp program permitted "no greater access to other users' shared files than any other Gnutella client" in holding that defendant "had no reasonable expectation of privacy over the files shared with Gnutella and, therefore, the use of the RoundUp program could not have violated his Fourth Amendment rights." *United States v. Brashear*, 2013 WL 6065326, at *3 (M.D. Pa. Nov. 18, 2013). *See also United States v. Thomas*, 2013 WL 6000484, at *17-18 (D.Vt. Nov. 8, 2013) ("the evidence overwhelming demonstrates that the only information accessed was made publicly available by the IP address or the software it was using. Accordingly, either intentionally or inadvertently, through the use of peer-to-peer file sharing software, Defendants exposed to the public the information they now claim was private. … A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *United States v. Dodson*, 960 F.Supp.2d 689, 694-95 (W.D. Tex. 2013) (government use of software program to assist in P2P investigation did not constitute a search because it only obtained publically shared information, and "a user of file-sharing software has no reasonable expectation of privacy in his

publicly shared files because it is not an expectation of privacy that society is willing to recognize").

Feldman was sharing child exploitation files with anyone who searched for those files on a P2P network, a process that does not require the use of proprietary law enforcement technology. Whether law enforcement's investigative techniques allowed for more efficient identification of those, like Feldman, who chose to publicly share child exploitation files is of no relevance to whether Feldman had a constitutionally-protected expectation of privacy in the files he chose to make widely available. Defendant's argument is akin to claiming that a stake out in which law enforcement observes an open-air drug transaction on a public street corner violates the drug dealer's right to privacy because most private citizens lack the time and resources to conduct a stake out, or the specialized knowledge to understand all the nuances of a drug transaction. Accordingly, Feldman has failed to articulate any reasonable privacy interest implicated by law enforcement's use of the *Roundup eMule* tool.

3. The search warrant established probable cause to search Feldman's residence.

Feldman also asserts, without any further explanation, that the search warrant affidavit "did not sufficiently allege probable cause." Motion to Suppress Memorandum at p. 1. "A search warrant affidavit establishes probable cause when it sets forth facts sufficient to induce a reasonable prudent person to believe that a search thereof will uncover evidence of a crime." *United States v. Jones* 208 F.3d 603, 608 (7th Cr. 2000) (internal quotations and citations omitted). "Probable cause for a search is far short of certainty; it requires only a probability or substantial chance of criminal activity, not an actual showing of such activity, and not a probability that exceeds 50 percent either." *United States v. Seiver*, 692 F.3d 774 (7th Cir.

2012). "[I]n child pornography cases, an issuing judge may reasonably assume that a recipient or collector of child pornography would store that content in his home." *United States v. Clark*, 668 F.3d 934, 943 (7th Cir. 2012). Nothing in defendant's motion, or in any of his supporting exhibits, calls into question the key facts underlying the question of probable cause. *Cf.* Case Recommendation at p. 11 (Ex. H hereto) (rejecting defendant's identical argument in closely analogous circumstances). The search warrant explains that an IP address which resolved to defendant's residence shared with the general public 17 files which generated the same hash values as known child exploitation files. An investigator personally confirmed that those known child exploitation files depicted children engaged in sexually explicit conduct, and described the conduct depicted in two of those files in the search warrant affidavit.

Here, the facts described in the affidavit easily exceed the probable cause threshold. And indeed, courts across the country have repeatedly affirmed findings of probable cause to search a residence under essentially identical circumstances. *See, e.g.*, *Miknevich*, 638 F.3d at 184; *United States v. Beatty*, 437 Fed. App'x 185, 186–88 (3d Cir. 2011) (finding a sufficient showing of probable cause where officer did not open and view the suspect files, but explained the file retrieval process, provided the names of suspect files, and cross-referenced and matched each file's SHA1 value to known child pornography files contained in a database maintained by the Wyoming Internet Crimes Against Children Task Force); *United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (affirming district court ruling that hash value matching alone established probable cause for issuance of a search warrant); *United States v. Bershchansky*, 958 F.Supp.2d 354, 358 (E.D.N.Y. 2013) (finding a sufficient showing of probable cause where officer did not download any child exploitation files, but did confirm based on SHA1 matching that defendant

was offering to share child pornography); *United States v. Willard*, 2010 WL 3784944, at *1 n. 1 & *5 (E.D.Va. Sept. 20, 2010) (holding that"[b]y comparing the SHA1 values of two files, investigators can determine whether the files are identical with precision greater than 99.9999 percent certainty" and rejecting request for Franks hearing based upon a claim "that the officers making the affidavit made false statements regarding the accuracy of SHA1"); *United States v. Schmidt*, 2009 WL 2836460, at*7 (E.D. Mo. Aug. 27, 2009) (finding sufficient probable cause for search warrant based on police obtaining a list IP addresses that were offering a video file that was known to include child exploitation files, based on the video's SHA1 value, one of which resolved to defendant's residence).

4. Even if the search warrant was not supported by probable cause, the good-faith exception to the exclusionary rule applies.

Even if a search warrant was invalid because the supporting affidavit failed to support a finding of probable cause, evidence seized in executing the warrant should not be suppressed if the police officers relied in good faith on the judge's decision to issue the warrant. *United States v. Miller*, 673 F.3d 688, 693–94 (7th Cir.2012), citing *United States v. Leon*, 468 U.S. 897, 922–23 (1984). A police officer's decision to obtain a warrant is treated as prima facie evidence that the officer was acting in good faith. *United States v. Garcia*, 528 F.3d 481, 487 (7th Cir.2008). A defendant can defeat the good-faith exception to the exclusionary rule by showing (1) that the issuing judge abandoned the detached and neutral judicial role; (2) that the officer was dishonest or reckless in preparing the affidavit; or (3) that the warrant was so lacking in probable cause that the officer could not reasonably rely on the judge's issuance of it. *Id.*; *see also Leon*, 468 U.S. at 923. Where, like here, there is no indication that the issuing judge merely rubber-stamped the affidavit or that the officer preparing the affidavit was dishonest or reckless, the question of good

faith turns on whether the warrant was so facially deficient that an officer could not reasonably rely on it. *Miller*, 673 F.3d at 693. As discussed in great detail above, courts throughout the country have repeatedly held that search warrants presenting facts virtually identical to the instant warrant established probable cause to search a defendant's residence, and execution of those warrants regularly resulted in seizure of contraband child exploitation files. Accordingly, the executing officers reasonably relied upon a search warrant that mirrored a long line of on-point precedent.

III. CONCLUSION

This case is not complicated. Agents conducted an online investigation into the sharing of child exploitation files over a public file-sharing network. Through this investigation, agents observed child exploitation files shared publicly from a computer using an IP address that was indisputably tied to Jeffrey Feldman. Based upon this information, which in no way implicated any reasonable privacy interest, the affiant sought and obtained a warrant to search Jeffrey Feldman's house for evidence of child pornography.

Feldman's motion seeks suppression under *Franks v. Delaware*. The focus is on the veracity of the search warrant affidavit and the conduct of the affiant. Therefore, the law requires at the outset that Feldman make a "*substantial preliminary showing*" that an evidentiary hearing will expose the search warrant affidavit as intentionally or recklessly false. He has not, and cannot, do so. In fact, it is apparent from the content of the motion that Feldman seeks a *Franks* hearing in order to try to substantiate his speculative assertions. Such an approach is never warranted, and for the reasons set forth above, the United States respectfully requests that

the Court deny Feldman's request for a *Franks* hearing and deny Feldman's motion to suppress evidence.

In addition, Feldman's motion to compel discovery should be summarily denied. The government's extensive discovery production, including pointed responses to defendant's multiple lengthy discovery demands as well as making available for defense review the terabytes of computer forensic evidence seized from Feldman, more than satisfied the government's obligations under Fed. R. Crim P. 16. Rather than avail himself of offers from the United States to meet and confer to further discuss discovery, defendant has repeatedly brought motions to compel discovery.

Dated at Milwaukee, Wisconsin, this 24th day of March, 2014.

Respectfully submitted,

JAMES L. SANTELLE
United States Attorney

By: s/ Karine Moreno-Taxman

KARINE MORENO-TAXMAN
Assistant United States Attorney
Karine Moreno-Taxman Bar No.:1006835
Attorney for Plaintiff
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Ave. Suite 530
Milwaukee, Wisconsin 53202
Tel: 414-297-1785
Fax: 414-297-1783
Email: Karine.Moreno-Taxman@usdoj.gov

Jeffrey Zeeman
Trial Attorney
United States Department of Justice
1400 New York Avenue NW

Washington, DC 20005
Tel: (202) 514-6037
Fax: (202) 514-1793
Email: Jeffrey.Zeeman@usdoj.gov